漫遊連線機制建置說明手冊

OPENVPN & Freeradius

On CentOS7 with Ldap

一、 OpenVPN

1. 安裝套件 epel-release、openvpn

```
[root@openvpn]# yum install -y epel-release
[root@openvpn]# yum install -y openvpn
```

2. 將漫遊中心提供的 key 「clt_number_shortname.tar」放置/etc/openvpn 解壓縮

```
[root@openvpn]# cd  /etc/openvpn
[root@openvpn]# tar -zxf clt_number_shortname.tar
```

3. 複製服務啟動檔

```
[root@openvpn]# cp client.conf server.conf
```

4. 啟動服務

```
[root@openvpn]# systemctl  restart  openvpn@server
```

5. 看 tun0 VPN 通道是否有啟動，如 tun0 有產生 10.1.X.X 代表 VPN 連線成功

```
[root@openvpn]# ifconfig tun0
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
        inet 10.1.X.X  netmask 255.255.255.255  destination 10.1.0.2
        inet6 fe80::ab85:e6d5:df58:63c9  prefixlen 64  scopeid 0x20<link>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 100
(UNSPEC)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3  bytes 144 (144.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

6. 設定開機啟動服務

```
[root@openvpn]# systemctl  enable  openvpn@server
```

二、 Freeradius

1. 安裝套件 freeradius freeradius-utils

```
[root@freeradius]# yum install -y freeradius freeradius-utils
```

2. 修改/etc/raddb 的 clients.conf 檔案

```
[root@freeradius]# cd    /etc/raddb
[root@freeradius]# vim clients.conf
              <--於檔案最後處加入下列內容-->
client 10.1.0.7 {
              secret          =    niucltcc
              shortname    =    niu
       }
client 10.1.0.11 {
               secret          =    niucltcc
               shortname    =    niu-roaming-monitor
}
```

3. 修改/etc/raddb 的 proxy.conf 檔案

```
[root@freeradius]# vim proxy.conf
              <--於檔案最後處加入下列內容-->
realm NULL {       #當遇到帳號並沒有 realm 時的預設動作為以本機進行認證動作
            authhost = LOCAL
            accthost = LOCAL
            secret = niucltcc
}

realm DEFAULT { #當遇到帳號帶有 realm 時的預設動作為送至漫遊中心進行 proxy 動作
            authhost = 10.1.0.7:1812
            accthost = 10.1.0.7:1813
            secret = niucltcc
            nostrip
}
```

4. 啟動服務

```
[root@freeradius]# systemctl  restart  radiusd
```

5. 測試 freeradius 驗證是否正常

```
[root@freeradius]# radtest  testuser@niu  testpass  127.0.0.1  0  testing123
                          < radtest  帳號  密碼  測試伺服器  測試伺服器之通訊埠  Secret >
Sending Access-Request of id 234 to 10.1.0.7 port 1812
        User-Name = "testuser@niu"
        User-Password = "testpass"
        NAS-IP-Address = 127.0.0.1
        NAS-Port = 0
rad_recv: Access-Accept packet from host 10.1.0.7 port 1812, id=234, length=20
```

6. 設定開機啟動服務

```
[root@openvpn]# systemctl  enable  radiusd
```

三、 Ldap 模組(網頁認證)

1. 安裝套件 freeradius-ldap 套件

```
[root@freeradius]#yum install freeradius-ldap
```

2. 修改 ldap 模組

```
[root@freeradius]#vim  /etc/raddb/mods-enabled/ldap

        server = IP address
        port = 389
        identity = 'cn=XXX,dc=XXX,dc=XXX,dc=XXX'
        password = PASSWD
        base_dn = ' dc=XXX,dc=XXX,dc=XXX'
```

3. 修改 default 檔案，新增判斷式

```
[root@freeradius]#vim  /etc/raddb/sites-enabled/default

authorize {
...略...
```

```
        if (!control:Auth-Type && User-Password) {
                update {
                        control:Auth-Type := ldap
                }
        }
...略...
}

authenticate {
...略...
        Auth-Type LDAP {
                ldap
        }
...略...
}
```

四、 Ldap 模組(EAP-802.1X)

1. 修改 inner-tunnel 檔案，新增判斷式

```
[root@freeradius]#vim   /etc/raddb/sites-enabled/inner-tunnel

authenticate {
…略…
        Auth-Type LDAP {
                ldap
        }
…略…
}
```

2. 修改 EAP 認證方式

```
[root@freeradius]#vim   /etc/raddb/mod-enabled/eap

eap {
…略…
    #default_eap_type = md5
    default_eap_type = peap
    gtc {
    …略…
            #auth_type = PAP
            auth_type = ldap
    …略…
    }
    peap{
    …略…
            #default_eap_type = mschapv2
            default_eap_type = gtc
    …略…
}
```